

AN APPLICATION OF THE DEDEKIND-HASSE CRITERION

F. LEMMERMEYER

ABSTRACT. In this article we show how the Dedekind-Hasse criterion may be applied to prove a simple result about quadratic number fields that usually is derived as a consequence of the theory of ideals and ideal classes.

INTRODUCTION

Let m be a squarefree integer, $K = \mathbb{Q}(\sqrt{m})$ the quadratic number field generated by the square root of m , D_m its ring of integers, and $\Delta = \text{disc}K$ its discriminant. The following result is called the

Theorem 1 (Dedekind-Hasse Criterion). *The domain D_m is a principal ideal domain if for all $\alpha, \beta \in D_m \setminus \{0\}$ with $\beta \nmid \alpha$ and $|N\alpha| \geq |N\beta|$ there exist $\gamma, \delta \in D_m$ such that*

$$0 < |N(\alpha\gamma - \beta\delta)| < |N\beta|. \quad (1)$$

Actually, this is only a very special case of Dedekind's and Hasse's result, who considered more generally arbitrary number fields and even general rings.

For squarefree integers m as above we define the Gauss bound

$$\mu_m = \begin{cases} \sqrt{-\Delta/3} & \text{if } m < 0, \\ \sqrt{\Delta/5} & \text{if } m > 0. \end{cases}$$

In this note¹ we will show how to use the Dedekind-Hasse criterion for proving the following

Theorem 2. *Assume that for all rational primes p with $2 \leq p \leq \mu_m$ with $(\frac{\Delta}{p}) \neq -1$ there is an element $\pi \in D_m$ with $p = |N\pi|$, then D_m is a PID.*

In the case $m < 0$, no prime $p < \mu_p$ can be a norm from D_m , and we obtain the

Corollary 3. *Assume that $m < 0$ and $(\frac{\Delta}{p}) = -1$ for all prime numbers p with $2 \leq p \leq \sqrt{-\Delta/3}$; then D_m is a PID.*

In particular, D_m is a PID for $-m = 1, 2, 3, 7, 11, 19, 43, 67, 163$.

It is also easy to see that Thm. 2 holds whenever D_m is a unique factorization domain; thus we find

Corollary 4. *A number ring D_m is a UFD if and only if it is a PID.*

¹This note was written around 1985.

1. PROOF OF THE MAIN THEOREM

Since $N\beta \neq 0$, the condition (1) is equivalent to

$$0 < |N(\xi\gamma - \delta)| < 1 \quad \text{for all } \xi = \frac{\alpha}{\beta} = \frac{a + b\sqrt{m}}{c} \in K \setminus D_m; \quad (2)$$

the exclusion of $\xi \in D_m$ comes from the condition that $\beta \nmid \alpha$. Write $\xi = \frac{a+b\sqrt{m}}{c}$ for integers a, b, c with $c \geq 2$. Without loss of generality we may assume that $\gcd(a, b, c) = 1$.

Lemma 5. *It is sufficient to prove (2) for prime values of c .*

Proof. Assume that $c = c_1 c_2$ is a factorization of c with $c_1, c_2 \geq 2$. Then at least one of $\frac{a+b\sqrt{m}}{c_1}$ or $\frac{a+b\sqrt{m}}{c_2}$ is not in D_m unless $c_1 = c_2 = 2$, $m \equiv 1 \pmod{4}$, and $a \equiv b \pmod{2}$. We treat these cases separately.

$\frac{a+b\sqrt{m}}{c_1} \in K \setminus D_m$. Assume that we can find $\gamma_1, \delta \in D_m$ with

$$0 < \left| N\left(\frac{a+b\sqrt{m}}{c_1}\gamma_1 - \delta\right) \right| < 1.$$

Setting $\gamma = c_2\gamma_1$ we find

$$0 < \left| N\left(\frac{a+b\sqrt{m}}{c}\gamma - \delta\right) \right| < 1$$

as desired.

$m \equiv 5 \pmod{8}$, $c = 4$, $a \equiv b \equiv 1 \pmod{4}$. Since $a^2 - mb^2 \equiv 4 \pmod{8}$ there is an integer δ with $a^2 - mb^2 = 8\delta + 4$. Set $\gamma = \frac{a-b\sqrt{m}}{2}$; then

$$N(\xi\gamma - \delta) = N\left(\frac{1}{2}\right) = \frac{1}{4},$$

hence (2) is satisfied.

$m \equiv 1 \pmod{8}$, $c = 4$, $a \equiv b \equiv 1 \pmod{4}$. Then $(\frac{\Delta}{2}) = +1$, hence there is nothing to prove in the case $\Delta < 0$ and $2 < \sqrt{-\Delta/3}$. In the remaining cases there exists an element $\pi = \frac{x+y\sqrt{m}}{2}$ with $|N(\pi)| = 2$:

- $m < 0$, $2 > \sqrt{-\Delta/3}$: then $m = -7$, and we can take $x = y = 1$.
- $m > 0$, $2 > \sqrt{\Delta/5}$: then $m = 17$, and we can take $x = 5$, $y = 1$.
- $m > 0$, $2 < \sqrt{\Delta/5}$: here the existence follows from the assumption of the theorem.

Now set $\gamma = 1$ and $\delta = \frac{1}{2}(\frac{a-x}{2} + \frac{b-y}{2}\sqrt{m})$; then $\xi\gamma - \delta = \frac{x+y\sqrt{m}}{4} = \frac{\pi}{2}$, hence $0 < |N(\xi\gamma - \delta)| = |N(\frac{\pi}{2})| = \frac{1}{2} < 1$ as desired.

This finishes the proof of Lemma 5. □

Our next result is

Lemma 6. *It is sufficient to verify (2) for $c < \mu_m$.*

Proof. Since $\gcd(a, b, c) = 1$ there exist integers d, e, f with $ad + be + cf = 1$. We distinguish two cases.

1. $m \equiv 2, 3 \pmod{4}$. By division with remainders in the rational integers there exist integers q, r with

$$ae + mbd = cq + r, \quad \text{where} \quad \begin{cases} 0 \leq |r| \leq \frac{c}{2} & \text{if } m < 0, \\ \frac{c}{2} \leq |r| \leq c & \text{if } m > 0. \end{cases}$$

Setting $\gamma = e + d\sqrt{m}$ and $\delta = q - f\sqrt{m}$ we find

$$\xi\gamma - \delta = \frac{(ae + mbd - cq) + (ad + be + cf)\sqrt{m}}{c} = \frac{r + \sqrt{m}}{c},$$

hence $N(\xi\gamma - \delta) = \frac{r^2 - m}{c^2}$.

- If $m < 0$ and $c > \sqrt{-\Delta/3} = \sqrt{-4m/3}$, then

$$0 < N(\xi\gamma - \delta) = \frac{r^2 - m}{c^2} = \frac{r^2 + |m|}{c^2} < \frac{c^2 + 3c^2}{4c^2} = 1.$$

- If $m > 0$ and $c > \sqrt{\Delta/5} = \sqrt{4m/5}$, then

$$0 < N(\xi\gamma - \delta) = \frac{r^2 - m}{c^2} \quad \begin{cases} \geq \frac{(c/2)^2 - m}{c^2} > -1, \\ < \frac{r^2}{c^2} \leq 1. \end{cases}$$

This finishes the proof of Lemma 6 in the case $\Delta = 4m$.

2. $m \equiv 1 \pmod{4}$. We claim that we can choose the integers d, e, f with $ad + be + cf = 1$ in such a way that $d \equiv e \pmod{2}$. In fact, if $d \equiv e + 1 \pmod{2}$ then either c is odd or $c = 2$ (by Lemma 5). If c is odd we set $e' = e + c$ and $f' = f - b$; then $ad + be' + cf' = 1$ and $d \equiv e' \pmod{2}$. If $c = 2$ we must have $a \equiv b + 1 \pmod{2}$ (otherwise $\xi \in D_m$) and set $d' = b + d$ and $e' = e - a$; then $ad' + be' + cf = 1$ and $d' \equiv e' \pmod{2}$.

Now there are integers q, r with $ae + mbd = cq + r$, where we choose r in such a way that $q \equiv f \pmod{2}$ and

$$\begin{cases} 0 \leq |r| \leq c & \text{if } m < 0, \\ c \leq |r| \leq 2c & \text{if } m > 0. \end{cases}$$

Setting $\gamma = \frac{e + d\sqrt{m}}{2} \in D_m$ and $\delta = \frac{q - f\sqrt{m}}{2} \in D_m$ we verify (2) exactly as in the case $m \equiv 2, 3 \pmod{4}$. \square

The final step in the proof of Thm. 2 is

Lemma 7. *It is sufficient to verify (2) in the case where $c = p$ is prime with $a^2 - mb^2 \equiv 0 \pmod{p}$ and $(\frac{\Delta}{p}) \neq -1$.*

Proof. Assume that $c \nmid (a^2 - mb^2)$; then $a^2 - mb^2 = cq + r$ for integers q, r with $0 < |r| \leq \frac{c}{2}$, and we set $\gamma = a - b\sqrt{m}$ and $\delta = q$. Then we obtain

$$\xi\gamma - \delta = \frac{a^2 - mb^2}{c} - q = \frac{r}{c} \neq 0,$$

and the inequalities (2) are easily verified.

If $(\frac{\Delta}{c}) = -1$, the congruence $a^2 - mb^2 \equiv 0 \pmod{c}$ is not solvable for odd primes c . If $c = 2$, on the other hand, then $(\frac{\Delta}{c}) = -1$ implies $\Delta = m \equiv 5 \pmod{8}$, and $a \equiv b \equiv 1 \pmod{2}$ implies $\beta \mid \alpha$. \square

For the proof of Thm. 2 it remains to take care of the prime values $c = p < \mu_m$ with $p \mid \Delta$ or $(\frac{\Delta}{p}) = +1$. By assumption there is an element $\pi \in D_m$ with $|N\pi| = p$. For negative discriminants this is impossible, hence we only have to consider the case $m > 0$. We have to show that we can satisfy (2) for primes $c = p$ with $p \mid \Delta$.

1. The case $c = 2$. If $m \equiv 1 \pmod{4}$, then $a^2 - mb^2 \equiv 0 \pmod{2}$ implies $a \equiv b \pmod{2}$, hence $\beta \mid \alpha$ and $\xi \in D_m$.

If $m \equiv 2, 3 \pmod{4}$, $a^2 - mb^2 \equiv 0 \pmod{2}$ and $c < \sqrt{4m/5}$, then there is a $\pi = x + y\sqrt{m} \in D_m$ with $2 = |x^2 - my^2|$. We easily check that $a \equiv x$ and $b \equiv y \pmod{2}$, and by setting $\gamma = 1$ and $\delta = \frac{a-x}{2} + \frac{b-y}{2}\sqrt{m} \in D_m$ we find

$$|N(\xi\gamma - \delta)| = \left| \frac{x^2 - my^2}{4} \right| = \frac{1}{2}$$

as desired.

2. The case $c = p$ for odd primes p . Assume that $c = p$ is an odd prime, $m > 0$, $a^2 - mb^2 \equiv 0 \pmod{p}$ and $p < \sqrt{\Delta/5}$. By assumption there is a $\pi = \frac{x+y\sqrt{m}}{2} \in D_m$ with $|N\pi| = p$.

Case I. $p \nmid m$. If we had $p \mid a$, then we also would have $p \mid b$ (and conversely), hence $\beta \mid \alpha$. Thus $p \nmid ab$. From $p = |\frac{x^2 - my^2}{4}|$ we deduce that $x^2 \equiv my^2 \pmod{p}$; since we also have $a^2 \equiv mb^2 \pmod{p}$ we must have $\frac{x}{2a} \equiv \pm \frac{y}{2b} \pmod{p}$. Replacing y by $-y$ if necessary we may assume that, in this congruence, the plus sign holds; letting z denote an integer with $z \equiv \frac{x}{2a} \pmod{p}$ we find

$$(a + b\sqrt{m})z \equiv \frac{x + y\sqrt{m}}{2} = \pi \pmod{p}.$$

Thus there is a $\delta \in D_m$ with $(a + b\sqrt{m})z = \pi + p\delta$. We now set $\gamma = z$ and find

$$\xi\gamma - \delta = \frac{a + b\sqrt{m}}{p}z - \delta = \frac{x + y\sqrt{m}}{2p},$$

which immediately shows that (2) is satisfied.

Case II. $p \mid m$. Since $p \mid (a^2 - mb^2)$ we must have $p \mid a$. As before, $p \mid b$ would imply $\beta \mid \alpha$, hence $p \nmid b$. Since m is squarefree, we must have $p^2 \nmid (a^2 - mb^2)$, i.e., $\gcd(\frac{a^2 - mb^2}{p}, p) = 1$. Thus there exist integers r, s with

$$\frac{a^2 - mb^2}{p} \cdot r + ps = 1. \tag{3}$$

Since $p \mid m$, the prime p ramifies in D_m , hence $\pi \mid \sqrt{m}$ and therefore $\pi \mid a - b\sqrt{m}$ since $p \mid a$. Dividing (3) through by π we find

$$\frac{a + b\sqrt{m}}{p} \cdot \frac{a - b\sqrt{m}}{\pi} \cdot r \pm \bar{\pi}s = \frac{1}{\pi},$$

where $\bar{\pi}$ is the conjugate of π and thus satisfies $\pi\bar{\pi} = N\pi = \pm p$. Setting $\gamma = \frac{a - b\sqrt{m}}{\pi} \cdot r$ and $\delta = \pm \bar{\pi}s$ we find that (2) is satisfied.

This finishes the proof of Theorem 2.

2. APPLICATIONS

Assume now that D_m is a UFD. Then for all $\alpha, \beta \in D_m$ there exists a $\rho \in D_m$ with $(\rho) = (\alpha, \beta)$, and $\lambda, \mu \in D_m$ with

$$\alpha\lambda + \beta\mu = \rho. \quad (4)$$

In this section we will show that there is an algorithm for computing a Bezout representation (4) using the Euclidean algorithm in \mathbb{Z} and the prime elements π in Theorem 2 whose norms lie below the Gauss bound.

In fact, given α and β as above we can compute, as in the proof of Theorem 2, elements $\gamma_0, \delta_0 \in D_m$ with $\rho_1 = \alpha\gamma_0 - \beta\delta_0$ and $0 < |N\rho_1| < |N\beta|$. If $\rho_1 \mid \beta$, then we also have $\rho_1 \mid \alpha$, and it follows that $(\alpha, \beta) = (\rho_1)$, and that (4) holds with $\lambda = \gamma_0$ and $\mu = \delta_0$.

If $\rho \nmid \beta$, then $|N\rho_1| < |N\beta|$ shows that we can apply Thm.2 to the pair (β, ρ) , and we can find $\gamma_1, \delta_1 \in D_m$ with

$$\rho_2 = \beta\gamma_1 - \rho_1\delta_1, \quad 0 < |N\rho_2| < |N\rho_1|.$$

If $\rho_2 \mid \rho_1$, then $(\alpha, \beta) = (\rho_2)$, and (4) holds with $\lambda = -\gamma_0\delta_1$ and $\mu = \gamma_1 + \delta_0\delta_2$.

If $\rho_2 \nmid \rho_1$ we can apply Thm. 2 again; since the norm cannot decrease indefinitely, we eventually must find that $\rho_n \mid \rho_{n-1}$. Then $(\alpha, \beta) = (\rho_n)$, and by working backwards we find, in the usual way, the Bezout elements λ and μ .

Computing Prime Elements. Assume that p is a prime with $p > \mu_m$, and that we know an integer x with $x^2 \equiv m \pmod{p}$. If D_m is a UFD, then we can compute an element $\pi \in D_m$ with $|N\pi| = p$ as follows: set $\alpha = p$ and $\beta = x - \sqrt{m}$; then $(\pi) = (\alpha, \beta)$ for some $\pi \in D_m$ with norm $\pm p$.

Example. Let $m = 14$, $p = 137$, $x = 39$; then $\alpha = 137$ and $\beta = 39 - \sqrt{14}$. We find $\frac{137}{39 - \sqrt{14}} = \frac{39 + \sqrt{14}}{11}$, hence $a = 39$, $b = 1$, $c = 11$; we choose $d = 0$, $e = 12$, $f = -1$ and find $ad + be + cf = 1$. Moreover $ae = 468 = qc + r = 43 \cdot 11 - 5$, hence $q = 43$ and $r = -5$ (we choose r in such a way that it minimizes $|r^2 - m|$), and $\gamma_0 = 12$, $\delta_0 = 43 + \sqrt{14}$. Thus we find

$$\begin{aligned} \rho_1 &= \alpha\gamma_0 - \beta\delta_0 = 137 \cdot 12 - (39 - \sqrt{14})(43 + \sqrt{14}) \\ &= -19 + 4\sqrt{14}. \end{aligned}$$

Since $\frac{\beta}{\rho_1} = -5 - \sqrt{14}$ we are already done:

$$(137, 39 - \sqrt{14}) = (-19 + 4\sqrt{14}),$$

and in fact we have $N(-19 + 4\sqrt{14}) = 137$.

REFERENCES

- [Ded] R. Dedekind, *Charakteristische Eigenschaft einfacher Körper*, Ges. Math. Werke II, 373–375
- [Has] H. Hasse, *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integritätsbereichen*, J. Reine Angew. Math. **159** (1928), 3–12

E-mail address: hb3@ix.urz.uni-heidelberg.de

MÖRIKEWEG 1, 73489 JAGSTZELL, GERMANY